REMARKS

Claims 66-102 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wagener (U.S. Pat. No. 5,793,028), Bramhill (WO 98/44402) and Wray (GB 2355322A).

The present invention, as defined by claim 66, relates to a network system. The network system includes first and second computer arrangements connected by a computer network. The second computer arrangement stores data and fingerprint software. The first computer arrangement is programmed to transmit a request for data to the second computer arrangement, receive fingerprint software from the second computer arrangement, execute the fingerprint software, and receive the requested data from the second computer arrangement. During the execution of the fingerprint software, fingerprint data that is substantially unique to the first computer arrangement is created and transmitted to the second computer arrangement. The second computer arrangement is programmed to receive a request for data from the first computer arrangement, transmit the fingerprint software to the first computer arrangement in response to receiving the request, receive fingerprint data from the first computer arrangement, and transmit the requested data to the first computer arrangement in response to receiving the fingerprint data.

Wagener describes a security system for performing electronic transactions. When an individual (transactionor) wishes to perform a transaction with another individual (transactionee), the security system first verifies, via a third individual (verifier), that the identities of the individuals are genuine. Each transactionor and transactionee is provided with a unique public identification code and a unique private identification code (col. 3, lines 37-58 of Wagener). The public identification code is used to identify each individual and is used by the security system for addressing purposes. For example, a transactionor uses the public identification code to specify that a transaction is to be carried out with the

transactionee having that particular public identification code. Whilst the public identification code is publicly available, the private identification code is known only to the transactionor or transactionee and to the verifier. Importantly, the private identification code of a transactionor is not known by the transactionee, and vice versa. The verifier is also provided with a public identification code, so that the verifier can be identified and addressed by both the transactionor and the transactionee.

Each individual is provided with a computer and consequently the security system may be regarded as comprising a transactionor computer, a transactionee computer and a verifier computer (col. 4, lines 32-59 of Wagener). In order to perform a transaction, the transactionor enters the details of the transaction into the transactionor computer. The transactionor computer then transmits a Transaction Initiation Request to the verifier computer (col. 5, lines 10-29). The Transaction Initiation Request includes the public identification codes of the transactionor and the transactionee such that the verifier computer is able to correctly identify the two individuals involved in the transaction. The verifier computer then transmits a Transaction Request to the transactionee computer. The Transaction Request includes the public identification code of the transactionor, such that the transactionee computer is able to identify the transactionor. In response to receiving a Transaction Request, the transactionee computer generates a Verification Request, which is returned to the verifier computer. The Verification Request includes the private identification code of the transactionee, which the verifier computer subsequently uses to verify that the identity of the transactionee is genuine. In response to receiving the Verification Request, the verifier computer transmits an Acknowledgement Request to the transactionor computer.

Upon receiving the Acknowledgement Request, the transactionor computer transmits an Acknowledgement Response to

the verifier computer. The Acknowledgement Response includes the private identification code of the transactionor, which the verifier computer subsequently uses to verify that the identity of the transactionor is genuine. Finally, the verifier computer checks, among other things, that the private identification codes received from the transactionor and the transactionee are valid (col. 7, lines 19-24 of Wagener). Upon verification, the verifier computer transmits a Verification Response to the transactionee computer, and the transaction between the transactionor computer and the transactionee computer proceeds.

With the security system described by Wagener, the verifier acts as an intermediary between the transactionor and the transactionee. Since the private identification codes are transmitted only from the transactionor to the verifier and from the transactionee to the verifier, the verifier is able to verify the identity of both the transactionor and the transactionee prior to a transaction being initiated. However, it is possible that an unauthorized person may gain access to an individual's private identification code. Accordingly, in order to further improve security, each individual (including the verifier) is provided with a unique authorization code, such as a password or customer-coded software or hardware (col. 4, lines 9-22). The identities of the transactionor and transactionee are then verified by the verifier only in the event that the private identification codes and the authorization codes are valid. Additionally, the transactionor and transactionee will only communicate with the verifier in the event that the authorization code of the verifier is valid.

The examiner alleges that Wagener describes a first computer that: transmits a request for data to a second computer; executes fingerprint software to create fingerprint data; transmits fingerprint data to the second computer; and receives the requested data. Additionally, the examiner alleges that Wagener describes a second computer that: stores a copy of the fingerprint software that is executed by the first computer;

receives from the first computer a request for data; transmits the fingerprint data to the first computer in response to receiving the request; receives fingerprint data from the first computer; and transmits the requested data to the first computer in response to receiving the fingerprint data.

The examiner makes no indication which computer of the security system is alleged to be equivalent to the first computer and which is alleged to be equivalent to the second computer. However, the transactionee computer sends a Verification Request to the verifier computer and in response the verifier computer performs a check and returns a Verification Response. Therefore, for the purposes of this discussion, applicant will assume the examiner considers the transactionee computer to be equivalent to the first computer and considers the verifier computer to be equivalent to the second computer. Applicant observes that the arguments presented below are equally applicable to other configurations.

Wagener therefore describes a transactionee computer that transmits a request for data (Verification Request) to the verifier computer. The request includes data (private identification code and authorization code) that uniquely identifies a user of the transactionee computer. The transactionee computer subsequently receives the requested data (Verification Response) from the verifier computer.

Although the transactionee computer of Wagener transmits data that uniquely identifies a user (i.e. private identification code and authorization code), the transactionee computer does not transmit data that uniquely identifies the computer. Consequently, the asserted equivalent to the first computer does not generate or transmit "fingerprint data" as that term is defined in claim 66. This point is acknowledged by the examiner in the office action.

Wagener states that the authorization code of a user may be generated using customer-coded software that is executed by the transactionee computer (col. 4, lines 9-22 of Wagener). The

customer-coded software is not, however, received from the verifier computer. Wagener therefore does not disclose that the transactionee computer is programmed to "receive fingerprint software" from the verifier computer. Again, this point is acknowledged by the examiner in the office action.

With the system of Wagener, the request for data (Verification Request) transmitted by the transactionee computer includes the authorization code of the user. In other words, the transactionee computer transmits a request for data that includes data that uniquely identifies a user. In contrast, the first computer of the present invention, as defined by claim 66, is programmed to "transmit a request for data," perform intermediate steps, and then "transmit the fingerprint data." Thus, the "request for data" and the "fingerprint data" are not transmitted together but are instead transmitted in two distinct steps.

The second computer (verifier computer) of Wagener may include customer-coded software that is executed by the second computer to generate an authorization code that is unique to the user of the second computer (col. 7, line 65 to col. 8, line 11 of Wagner). However, the customer-coded software of the second computer is clearly not the same as the customer-coded software of the first computer. The reason for this is that the customer-coded software generates an authorization code that is unique to a user using the computer. Consequently, the customer-coded software of the first and second computers must be different. In contrast, the second computer of the present invention stores a copy of the fingerprint software that is executed by the first computer.

In response to receiving the Verification Request from the transactionee computer, the verifier computer transmits a Verification Response, that includes the authorization code, to the transactionee computer. The transactionee computer does not, however, transmit the customer-coded software used to generate the authorization code. Contrastingly, in the present invention as defined by claim 66, the second computer is programmed to

transmit a copy of the fingerprint software to the first computer. The examiner appears to be of the opinion that Wagener describes an equivalent to the second computer that transmits an equivalent to the fingerprint software in response to receiving a request for data. However, applicant respectfully submits that this in incorrect. Wagner does not disclose any computer in the security system as transmitting software of any kind.

Wagener's verifier computer transmits the Verification Response to the transactionee computer in response to receiving a Verification Request that includes an authorization code. The verifier computer therefore receives the Verification Request along with the authorization code. In the present invention, as defined by claim 66, the second computer is programmed to "receive a request for data," transmit the fingerprint software to the first computer, and then subsequently, and separately, "receive fingerprint data from the first computer." Thus, the request for data and fingerprint data are not received together but are instead received in two distinct steps.

The security system described by Wagener therefore differs from the present invention, as defined by claim 66, in at least the following aspects:

(1) the asserted equivalent to the first computer (the transactionee computer) is not programmed to receive anything equivalent to the fingerprint software (as is acknowledged by the examiner);

(2) the customer-coded software executed by the transactionee computer does not generate anything equivalent to the fingerprint data (as is acknowledged by the examiner);

(3) even if the customer-coded software did generate an equivalent to the finger print data, the transactionee computer is not programmed to transmit a request for data and to then subsequently and separately transmit the "fingerprint data";

(4) the software stored by the second computer is different to the software executed by the first computer;

(5) the asserted equivalent to the second computer (the verifier computer) is not programmed to transmit software of any kind to the transactionee computer; and
(6) even if the customer-coded software did generate an equivalent to the finger print data, the verifier computer is not programmed to receive a request for data and to then subsequently and separately receive the "fingerprint data."

Bramhill describes a dogtag program that, when executed on a computer, creates a machine identification code that is unique to the computer (page 17, lines 1-4 of Bramhill). However, there is no motivation for a person having ordinary skill in the art to which the invention pertains to modify the security system of Wagener to use the dogtag program of Bramhill. In fact, such a modification would prevent the security system of Wagener from operating in the intended manner.

The intention of the security system of Wagener is to prevent the unauthorized use of an individual's credit card details for electronic transactions over the Internet (col. 1, lines 28-48). This is achieved through the use of an authorization code that is unique to an individual. If the customer-coded software of Wagener were replaced with the dogtag program of Bramhill, a code unique to an individual would no longer be generated and verified. Instead, the code would be unique to a computer. Replacing the customer-coded software with the dogtag program would therefore defeat the very intention of the security system of Wagener. Moreover, replacing the customer-coded software with the dogtag program would have two important implications. First, an individual would not be able to use any computer to perform a transaction. Instead, the individual would be capable of using only a computer whose unique machine identification code had been pre-registered with the verifier. Second, an unauthorized individual would be capable of performing an unauthorized transaction merely by using the same pre-registered computer.

Therefore, applicant submits it would not have been obvious to a person having ordinary skill in the art to which the invention pertains to modify the security system of Wagener such that the authorization code unique to an individual is replaced by a machine identification code that is unique to a computer.

Even if the skilled person were to replace the customer-coded program of Wagener with Bramhill's dogtag program, the dogtag program would neither be stored on the verifier computer nor transmitted to the transcactionee computer. Instead, the dogtag program would have to be preinstalled on the transactionee computer prior to a transaction taking place.

The examiner alleges that Wray teaches a system whereby fingerprint software is stored on a second computer and is transmitted to the first computer in response to a request for data. In particular, the examiner alleges that the receiving step 200 of Figure 8 and the setup step 400 of Figure 12 of Wray, as well as their respective explanations in the specification, teach such an arrangement.

Wray describes a system for positively identifying a client terminal that attempts to communicate with a host machine (e.g. page 15, lines 9-11 of Wray). The client terminal and the host machine respectively have EPCI software and ASR software installed thereon. The EPCI software creates a client identifier key (CIK), which includes data that are unique to the hardware and software configuration of the client terminal (page 29, lines 9-13).

When the client terminal attempts to communicate with the host machine, the ASR software requests that the CIK of the client terminal be returned. The EPCI software then creates a CIK for the client terminal and compares this against a previously-created CIK that is stored on the client terminal; this then prevents illegal copying of the EPCI software to a different client terminal. If the newly-generated CIK corresponds to the previously-created CIK, the EPCI software sends the newly-generated CIK to the host machine. The ASR

software is then able to positively identify the client terminal from the CIK (page 29, lines 9-15 of Wray).

The examiner appears to be under the impression that the EPCI software is stored on the host machine (the second computer) and then transmitted to the client terminal (the first computer) when the client terminal attempts to communicate with the host machine. However, applicant respectfully observes that this is not accurate. As is explained at page 35, lines 3-6 of Wray, the ASR software is installed on the host machine and the EPCI software is installed on the client terminal. There is no suggestion whatsoever of the EPCI software being stored on the host machine and being transferred to the client terminal in response to the host machine receiving a data request from the client terminal.

The examiner refers to step 200 of Figure 8 and step 400 of Figure 12 in the office action.

Figure 8 of Wray illustrates the steps followed by the EPCI software installed on the client terminal (e.g. page 39, lines 4-5 of Wray). Step 200 does not refer to the client terminal receiving the EPCI software from the host machine. Instead, step 200 refers to the EPCI software receiving a request from the ASR software of the host machine to send its unique CIK (e.g. page 39, lines 5-6 of Wray). In other words, step 200 refers to the client machine receiving a request to send its CIK. There is no suggestion of the EPCI software being stored and/or being transmitted by the host machine to the client terminal.

For the sake of completeness, particularly in view of the fact that the office action is final, applicant also observes that Wray makes reference to CIK generation software that is issued to the client terminal along with the EPCI software (e.g. page 26, lines 15-19). The CIK generation software is used to generate a first CIK for the client terminal. When the client terminal subsequently attempts to communicate with the host machine, the EPCI software generates a new CIK and compares this against the CIK created by the CIK generation software. As with

the EPCI software, the CIK generation software is not stored on the host machine, and it is not transmitted to the client terminal in response to the client terminal requesting data from the host machine.

Applicant therefore respectfully submits that the examiner's understanding of the disclosure of Wray is incorrect. In particular, applicant observes that Wray fails to teach or suggest a computer that stores fingerprint software and is programmed to transmit the software to a further computer in response to receiving a request for data.

Additionally, it is clear from Wagener that the Verification Request for data includes the transactionee's authorization code (Col. 6, lines 2-13), otherwise the request for data is treated as originating from a non-authorized computer. Applicant therefore submits that it would not have been obvious to a person having ordinary skill in the art to modify the security system of Wagener such that the transactionee computer (the asserted equivalent of the first computer) transmits a Verification Request and then subsequently and separately transmits an authorization code (the asserted equivalent of the finger print data). Moreover, there is no motivation for separately sending the request for data and the fingerprint data.

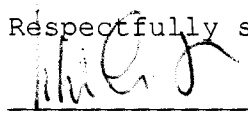
A particular problem with each of the systems described in the prior art cited by the examiner is that they require software to be preinstalled on the asserted equivalent to the first computer. Furthermore, the preinstalled software cannot be subsequently removed from the first computer. Therefore, it is not possible for an authorized individual to use an alternative computer without first installing the necessary software. In the case of Wagener, the customer-coded program must be installed on each of the transactionor, transactionee and verifier computers in order for the authorization codes to be generated, which are then included in the data requests and responses. In the case of Bramhill, the dogtag program must be installed and executed in

order to register the computer (page 17, line 20 of Bramhill) and then retained to subsequently self-authenticate prior to each data retrieval. In the case of Wray, the EPCI software must be installed and executed each time communication with the host machine is required.

In contra distinction, in the present invention, as defined by claim 66, the identity of a particular computer can be established without the need for preinstalled software. This is achieved by the means of fingerprint software that is stored on a server (second computer). When a client computer (first computer) requests data from the server, the server transfers the fingerprint software to the client computer. The fingerprint software is then executed by the client computer to create data that uniquely identifies the client computer. This fingerprint data is then returned to the server. Importantly, the data requested by the client computer is not delivered by the server until such time as the fingerprint data has been received. Accordingly, the identity of the client computer can be obtained immediately without requiring software to be preinstalled or retained on the client computer.

Applicant therefore submits that, for the reasons provided above, claim 66 of the present application is patentable. It follows that dependent claims 66-75 are also patentable. Applicant further submits that the above arguments are equally applicable to claims 76, 81, 90, 98 and 102 and therefore those claims are also patentable. It follows that dependent claims 77-80, 82-89, 91-97, and 99-101 are also patentable.

Respectfully submitted,



John Smith-Hill
Reg. No. 27,730

SMITH-HILL AND BEDELL, P.C.
16100 NW Cornell Road, Suite 220
Beaverton, Oregon 97006
Tel: (503) 574-3100
Fax: (503) 574-3197
Docket No. FORR 2276